

REMARKS

Please reconsider the application in view of the above amendments and the following remarks. Applicant thanks the Examiner for carefully considering this application.

Information Disclosure Statement

Applicant thanks the Examiner for initialing the IDS forms submitted on August 5, 2002, and June 9, 2003. Applicant respectfully requests that references A1 and A3 on the PTO Form-1449 from the IDS filed on June 9, 2003, be initialed and returned. If these Information Disclosure Statements have not been considered, appropriate consideration thereof is respectfully requested.

Disposition of Claims

Claims 1-29 were pending in the present application. By way of this reply, claims 14 and 28 have been cancelled without prejudice or disclaimer. Accordingly, claims 1-13, 15-27, and 29 are now pending in the present application. Claims 1, 15, and 29 are independent. The remaining claims depend, directly or indirectly, from claims 1 and 15.

Claim Amendments

Independent claims 1, 15, and 29 have been amended by way of this reply to require that data in the first Internet Protocol (“IP”) version compliant packet is encrypted using the security context, that the first IP version is different than the second IP version, and that data within the stripped packet is decrypted and authenticated using a particular method as indicated by the security context producing a decrypted and authenticated packet. No new matter has been

added by way of these amendments, as support for these amendments may be found, for example, in paragraphs [0031]-[0032] of the present application.

Rejection(s) under 35 U.S.C. § 102

Claims 1, 15, and 29 are rejected under 35 U.S.C. § 102(b) as being anticipated by the document titled “Network Working Group Request for Comments: 1241” by R. Woodburn and D. Mills (hereinafter “Woodburn”). Claims 1, 15, and 29 have been amended in this reply to clarify the present invention recited. To the extent that this rejection may still apply to the amended claims, the rejection is respectfully traversed.

The present invention is directed to a method for implementing a Supernet on a pre-existing IPv4 network, and using IPv6 in conjunction with IPv4 to convey a security context within a packet (*see, e.g.*, Specification, paragraph [0021]). As discussed with reference to an exemplary embodiment of the invention, a security context may include a Supernet ID, a channel ID, and a virtual network address (*see, e.g.*, Specification, paragraph [0021]).

Accordingly, amended independent claims 1, 15, and 29 require (i) creating and assigning a virtual address to a client process, (ii) issuing a first IP version compliant packet, where the first IP version compliant packet comprises a security context, and where data in the first IP version compliant packet is encrypted using the security context, and (iii) prepending an issued packet with a second IP version header producing a second IP version compliant packet, where the first IP version is different than the second IP version.

Woodburn, in contrast to the present invention, does not disclose creating and assigning a virtual address to a client process as required by the claimed invention. Woodburn is directed to an experimental protocol for Internet encapsulation. In contrast to the claimed invention, Woodburn discloses “a virtual interface whose sole purpose is encapsulation” (*see*

Woodburn, section D, page 15, paragraph 1). This virtual network overlays the actual routing topology. Further, although the Examiner has interpreted a user space as “any client, either a physical host or a process node having a physical or virtual address,” Woodburn has clearly defined a user space as the “address and routing space within which the users reside” (*see* Woodburn, section 2, page 3, paragraph 2). Clearly, a user space as taught by Woodburn does *not* refer to a client but rather to the space in which a user resides.

Further, Woodburn does not disclose issuing a first IP version compliant packet, where the first IP version compliant packet comprises a security context, and where data in the first IP version compliant packet is encrypted using the security context. As discussed above, a security context may include a Supernet ID, a channel ID, and a virtual network address. Woodburn is completely silent with respect to a security context. In fact, Woodburn clearly states that besides the checksum for the header information, no means of authentication or integrity checking is defined (*see* Woodburn, section F, page 17). To the extent that Woodburn discusses security, Woodburn suggests that authentication information be appended to the encapsulated datagram (*see* Woodburn, section F, page 17). It would be clear to one skilled in the art that Woodburn in no way contemplates a security context or that data in a first IP version compliant packet is encrypted using the security context. Arguably, Woodburn teaches away from the security offered by the claimed invention.

Further, Woodburn does not disclose prepending an issued packet with a second IP version header producing a second IP version compliant packet, where the first IP version is different than the second IP version. Woodburn is merely directed to encapsulation, or tunneling, within the Internet environment using “the current IP header format,” and providing a standard for performing encapsulation in the Internet environment (*see* Woodburn, section 3, page 3, paragraphs 4-5). Woodburn describes an encapsulation header, which consists of an IP

header and an encapsulation protocol header (*see* Woodburn, section 5, page 7, paragraph 8). However, in describing the basic concept of encapsulation, Woodburn is completely silent with respect to IP versions.

In view of the above, Woodburn fails to show or suggest the present invention as recited in amended independent claims 1, 15, and 29. Thus, amended independent claims 1, 15, and 29 are patentable over Woodburn. Accordingly, withdrawal of this rejection is respectfully requested.

Rejection(s) under 35 U.S.C. § 103

Claims 2-13 and 16-27

Claims 2-13 and 16-27 are rejected under 35 U.S.C. § 103(a) as being obvious over Woodburn in view of the document titled “IPv6: The New Protocol for Internet and Intranet” (hereinafter “Silvano”). Claims 1 and 15 have been amended in this reply to clarify the present invention recited. To the extent that this rejection may still apply to the amended claims, the rejection is respectfully traversed.

As discussed above, the present invention is directed to a method for implementing a Supernet on a pre-existing IPv4 network, and using IPv6 in conjunction with IPv4 to convey a security context within a packet. Further, as discussed above, amended independent claims 1, 15, and 29 require (i) issuing a first IP version compliant packet, where the first IP version compliant packet comprises a security context, and where data in the first IP version compliant packet is encrypted using the security context, and (ii) prepending an issued packet with a second IP version header producing a second IP version compliant packet, where the first IP version is different than the second IP version.

Woodburn, as discussed above, does not show or suggest the above limitations of the claimed invention. Silvano, as discussed above with reference to Woodburn, does not show or suggest that which Woodburn lacks. This is evidenced by the fact that Silvano is relied on only to teach limitations such as IP versions and the use of an authentication server daemon (*see* Office Action dated September 8, 2005, at page 7). Silvano is completely silent with respect to encapsulation using different IP versions. Thus, Silvano necessarily cannot show or suggest prepending an issued packet with a second IP version header to produce a second IP version compliant packet, where the first IP version is different than the second IP version.

Rather, Silvano is merely directed to the description of properties of IP version 6 (“IPv6”). Silvano compares different characteristics of IPv6 and IP version 4 (“IPv4”) and demonstrates the superior features of IPv6 over IPv4. However, Silvano is completely silent with respect to using these two different IP versions in conjunction with each other. While Silvano discusses security features of IPv6, Silvano focuses primarily on the Authentication Header (AH) and the Encrypted Security Payload (ESP) header. The AH header, as taught by Silvano, merely guards against illegal modification of fixed fields and packet spoofing. The ESP header, on the other hand, provides data encapsulation with encryption (*see* Silvano, section 8.1, page 153). In describing the ESP header, Silvano merely describes the known characteristics of the header, which is used to encrypt the upper level payload (*see* Silvano, section 8.1.3, page 156). Silvano describes an application of the AH and ESP headers to establish a virtual private network (VPN) (*see* Silvano, section 8.3.1, pages 160-162). However, like Woodburn, Silvano is completely silent with respect to *different* IP versions being used concurrently.

Further, Applicant notes that there is no motivation to combine the cited references. The Examiner cannot combine prior art references to render a claimed invention

obvious by merely showing that all the limitations of the claimed invention can be found in the prior art references. There must be a suggestion or motivation to combine the references within the prior art references themselves. In other words, regardless of whether prior art references can be combined, there must be an indication within the prior art references expressing desirability to combine the references. *In re Mills*, 916 F.2d 680 (Fed. Cir. 1990) (emphasis added). Further, the present application *cannot be used as a guide* in reconstructing elements of prior art references to render the claimed invention obvious. *In re Vaeck*, 947 F.2d 488 (Fed. Cir. 1991) (emphasis added).

One skilled in the art would not be motivated by Woodburn, which is directed to an experimental protocol for Internet encapsulation, and completely silent with respect to using IPv6 in conjunction with IPv4 to convey a security context within a packet, to incorporate the teachings of Silvano without the present application as a guide. The Examiner asserts that Woodburn provides suggestion to use, for example, IP versions 4 and 6, as well as a security context comprising a virtual address, a Supernet identity, and a channel identity. However, Woodburn is completely silent with respect to these limitations. Thus, one skilled in the art would not be motivated by Woodburn to incorporate the teaching of Silvano, which is solely directed to the IPv6 protocol. Further, Silvano is silent with respect to, for example, prepending an issued packet with a second IP version header producing a second IP version compliant packet, where the first IP version is different than the second IP version. One skilled in the art would not be motivated by Silvano, which is completely silent with respect to this limitation, to incorporate the teachings of Woodburn without the present application as a guide. Thus, there is no motivation to combine the cited references.

In view of the above, Woodburn and Silvano, whether taken separately or in combination, fail to show or suggest the present invention as recited in amended independent

claims 1 and 15, from which claims 2-13 and 16-27 depend. Thus, claims 2-13 and 16-27 are patentable over Woodburn and Silvano for at least the same reasons. Further, Woodburn and Silvano are not properly combinable. Accordingly, withdrawal of this rejection is respectfully requested.

Claims 14 and 28

Claims 14 and 28 are rejected under 35 U.S.C. § 103(a) as being obvious over Woodburn in view of the document titled “Mobile IPv6 Solution Based on Linux Netfilter Framework” by Gang *et al.* (hereinafter “Gang”). Claims 14 and 28 have been cancelled in this reply. Thus, the rejection with respect to claims 14 and 28 is now moot. Accordingly, withdrawal of this rejection is respectfully requested.

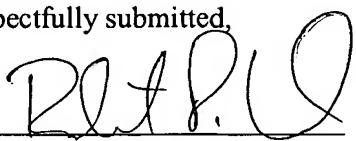
Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 16159/035001; P6566).

Dated: December 8, 2005

Respectfully submitted,

By



Robert P. Lord

Registration No.: 46,479

OSHA · LIANG LLP

1221 McKinney St., Suite 2800

Houston, Texas 77010

(713) 228-8600

(713) 228-8778 (Fax)

Attorney for Applicant

125162_2